Securing Open Source

Anil Saldhana

Red Hat Middleware (JBoss)

Anil.Saldhana@redhat.com

http://anil-identity.blogspot.com

DHS SwA Forum, Oct 14-16, 2008

National Institute of Standards and Technology (NIST)

redhat.

Speaker

- Lead Security Architect at Red Hat Middleware
- Participant in Standards efforts at W3C, Oasis and the Java Community Process (JCP)
- Open Source Champion (Bread and Butter)

redhat.

Ignorance

http://news.bbc.co.uk/2/hi/entertainment/7174760.stm

TV presenter Jeremy Clarkson *has lost money after publishing his bank details in his newspaper column*.

The Top Gear host revealed his account numbers after *rubbishing* the furore over the loss of 25 million people's personal details on two computer discs. He wanted to prove the story was a fuss about nothing.

But Clarkson *admitted he was "wrong"* after he discovered a reader had used the details to create a £500 direct debit to the charity Diabetes UK.

Is Ignorance bliss in a globally connected world operating at Internet Time?

Information aiding mass exploitation

http://en.wikipedia.org/wiki/Dan_Kaminsky

In July 2008, CERT announced that Kaminsky had discovered a *fundamental flaw in the DNS protocol itself*. The flaw could allow attackers to easily perform cache poisoning attacks on any nameserver.

Kaminsky had worked with DNS vendors in secret since earlier in the year to develop a patch to make exploiting the vulnerability more difficult, which was released on July 8, 2008. The vulnerability itself has not been patched, as it is a design flaw in the DNS itself.

Kaminsky had intended *not to* publicize details of the attack until 30 days after the release of the patch, but it was *accidentally leaked on July 21, 2008*. The leaked information was quickly pulled down, but not before it had been mirrored by others.

Prematurely leaked Sensitive information

redhat.

Open Source Software

http://en.wikipedia.org/wiki/Open_source_software

Open source software (OSS) began as a marketing campaign for free software.

OSS can be defined as computer software for which the *human-readable source code* is made available under a copyright license (or arrangement such as the public domain) that meets the Open Source Definition. This permits users to use, change, and improve the software, and to redistribute it in modified or unmodified form. It is very often developed in a public, collaborative manner.

Open Source Software

http://standishgroup.com/newsroom/open_source.php

"Open Source software is raising havoc throughout the software market," said Jim Johnson, Chairman, The Standish Group.

"It is the ultimate in *disruptive technology*, and while to it is only 6% of estimated trillion dollars IT budgeted annually, it represents a real loss of $60 billion in annual revenues to software companies," said Jim Johnson, Chairman, The Standish Group International, Boston, MA.

Prominent Open Source Software

- Apache Http Server (49% Marketshare, Netcraft, June08)
- Linux Operating System (7% Desktop, 12% Server) [IDC]
- JBoss Application Server
- Mozilla Firefox Browser (19% worldwide) [Browsers]
- OpenOffice (Alternative to Microsoft Office)
- Wordpress Blogging Software
- Apache Tomcat Servlet Container
- And thousands of them....

redhat.

Government involvement in OSS (Examples)

- NSA provides Security-Enhanced Linux
  - http://www.nsa.gov/selinux/
- DHS - “Open Source Hardening Project” - 2006
  - http://scan.coverity.com/
- GSA bets huge on Open Source
- http://anil-identity.blogspot.com/2008/04/us-federal-agency-gsa-bets-huge-on-open.html

“*The GSA heavily relies on open source to drive down costs, increase flexibility of IT dollars, and reduce risk.*”

- Casey Coleman, CIO, U.S. GSA

Views on Open Source Security

Topic: Keeping code secret or vulnerabilities secret

"*It's simply unrealistic to depend on secrecy for security in computer software. You may be able to keep the exact workings of the program out of general circulation, but can you prevent the code from being reverse-engineered by serious opponents? Probably not.*"

- Whitfield Diffie, co-inventor of public-key cryptography [Diffie]

redhat.

Is Open Source Secure?

- Software (closed or open source) is developed/supervised by humans
  - Prone to copy/paste errors, negligence, deadlines, budget etc
- So what would make Open Source Software secure?
  - Secure Practices (Development and Maintenance)
  - Backing from at least one professional company (stakeholder)
  - Customer demands for security related certifications
    - Common Criteria Evaluation, FIPS-140 etc
  - Documentation (Security Tuning, Best Practices)

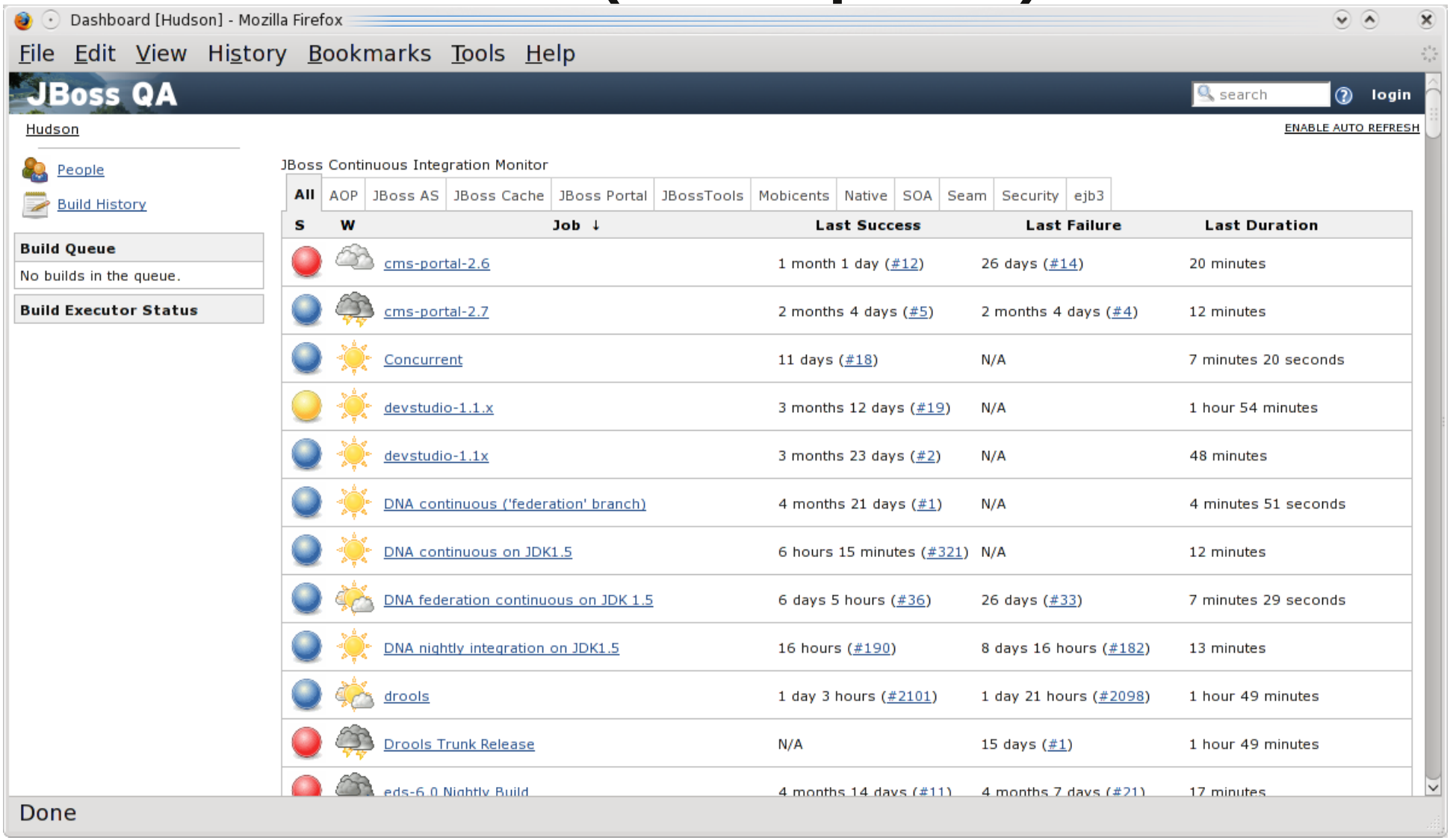
redhat.

Secure Practices (Development)

- Security experts on the development team
- Frequent code reviews by the team that is documented
  - Identifies patterns of potential errors among developers
- Use of automated tools
  - Static as well as dynamic analysis
  - Build setup (Cruisecontrol, Hudson are OSS examples)
  -

redhat.

Secure Practices (Development)



redhat.

Secure Practices (Maintenance)

- Security Vulnerabilities Reporting and Handling
  - Email or online contact form to report vulnerabilities
    - security@jboss.org
  - Unbiased vetting of the vulnerability and integration of the fix into the product
    - Project Lead/Senior Developers or dedicated security response team can vet
  - Based on severity of the vulnerability and the potential dangers if publicly reported, work with public vulnerability databases (CVE)
    - Inform your users/customers about the availability of fix
    - Ideally a test case that tests for the vulnerability needs to be incorporated to avoid regression

redhat.

Professional Companies' Stakeholders

- Apache HTTP Server, Linux, JBoss etc are incorporated into or sold as commercial solutions by companies
  - Real stake in the success/existence of the open source project
  - Every vulnerability or weakness in security in the project affects the financial bottom line
    - Employees of these companies participate in the development of the OSS leading to greater vigilance and adherence to standard practices in development and maintenance

Security Certification

- Platforms delivered on open source software get demands for certifications from customers (government/financial institutions)
  - Red Hat Enterprise Linux 5 is Common Criteria EAL4 certified
  - JBoss Enterprise Application Platform 4.3 currently under evaluation for EAL2
- Provide a feedback cycle into the OSS projects
- Security certification has external security evaluators evaluating source code, documentation, CVEs (Public Vulnerability Databases) and undertake independent vulnerability testing

Example of OSS Response [Linux]

- [CW] Mark Cox, who leads the Red Hat Security Response Team, says the responsiveness of any given open source project to a security issue depends on the project and the seriousness of the issue and many of the larger projects (for example, Apache, Mozilla, Linux kernel) have their own security response teams.
- For some issues, the finder of the vulnerability will contact the open source projects directly, and give them time to produce fixes before disclosing the issue publicly. In other cases, the open source project needs to react to an issue that is already public.
- "*A good example of reaction time was with a Linux kernel flaw On Saturday 9, February an exploit was made public that allowed a local unprivileged user to gain root privileges on some Linux kernels (CVE-2008-0600). Within a few hours of it being reported to the kernel mailing list, on 10 February, patches were being exchanged and tested. Later the same day the patches were committed and a new upstream kernel version was released*," says Cox.

Example of OSS Response [Linux]

- He adds that the benefit of using a Linux distribution is that security is managed by a single vendor, which can be preferable to having to subscribe to the security lists of all the different open source components being used.
- "*So Red Hat monitors a number of sources for details about security issues in any of the thousands of open source projects that make up our distributions, backport patches to correct the issues and release tested updates. Should an open source project not be responsive to a security issue, the vendors work together to come up with a peer-reviewed patch*," explained Cox.

redhat.

Reference Links

- [Browsers] http://en.wikipedia.org/wiki/Usage_share_of_web_browsers
- [Diffie] Risky business: Keeping security a secret (http://zdnet.com.com/2100-1107-980938.html)
- [IDC] Linux server market share keeps growing (http://www.linux-watch.com/news/NS5369154346.html)
- [CW] Open source software security (http://www.computerweekly.com/Articles/2008/04/18/229915/open-source-software-security.htm)

redhat.

Q&A